IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

ASHLEY POPA, *individually and on behalf of all others similarly situated*, *Plaintiff*, v. HARRIET CARTER GIFTS, INC. *a Pennsylvania corporation* and NAVISTONE, INC. *a Delaware corporation*, *Defendants*.	Civil Action No. 2:19-cv-450 Hon. William S. Stickman IV

OPINION

WILLIAM S. STICKMAN IV, United States District Judge

Plaintiff, Ashley Popa ("Popa"), brought this class action on behalf of herself and all others similarly situated against Defendants, Harriet Carter Gifts, Inc. ("Harriet Carter") and NaviStone, Inc. ("NaviStone") (collectively "Defendants"), alleging that they violated the Pennsylvania Wiretapping and Electronic Surveillance Control Act of 1978 ("WESCA"), 18 Pa. C.S. §§ 5703–5728, by unlawfully intercepting her data while she shopped online. (ECF No. 38, ¶¶ 1–2). In 2020, Defendants filed a motion for summary judgment, which this Court granted. (ECF Nos. 116, 117). The Court held that there was no interception under WESCA because NaviStone was a direct party to the communications. (ECF No. 116, p. 5). The Court also held that the alleged interception occurred outside of Pennsylvania and, thus, outside the scope of WESCA. (*Id.* at 15). The Court determined that NaviStone and Harriet Carter could not be liable to Popa under WESCA. (*Id.*).

Popa appealed, and the United States Court of Appeals for the Third Circuit reversed. The Third Circuit held that there is no "sweeping direct-party exception to civil liability under the WESCA," and that "NaviStone and Harriet Carter cannot avoid liability merely by showing that Popa unknowingly communicated directly with NaviStone's servers." (ECF No. 122-2, pp. 14-15). The Third Circuit further stated that "the place of interception is the point at which the signals were routed to NaviStone's servers," but that there was no source in the record regarding "where Popa's browser accessed the Harriet Carter website and where NaviStone's JavaScript began telling the browser to communicate with its servers." (*Id.* at 19-20). Thus, the matter was remanded to the Court to determine "whether there is a genuine issue of material fact about where the interception occurred." (*Id.* at 20).

The Third Circuit also noted that because the Court granted summary judgment on other grounds, it never addressed "whether Harriet Carter posted a privacy policy and, if so, whether that policy sufficiently alerted Popa that her communications were being sent to a third-party company." (*Id.* at 21). Thus, the matter of whether the Defendants are entitled to summary judgment on the basis of Harriet Carter's privacy policy was remanded to the Court. (*Id.* at 21-22). The issue of Harriet Carter's privacy policy is relevant to determining whether Popa consented to any interception under the provisions of WESCA.

After additional discovery, Defendants moved for summary judgment in their favor. (ECF No. 165).[1] Defendants take issue with the Third Circuit's interpretation of WESCA. They further

[1] Also pending before the Court is Popa's Motion to Strike Additional Opinions and Conclusions, and Related Exhibits, of Grigori (Greg) Humphreys Disclosed in his June 14, 2024, Declaration. (ECF No. 170). This motion will be denied. The Court holds that Humphrey's supplemental declaration is within the scope of his prior opinions and does not cause any prejudice to Popa. In any event, the declaration at issue is immaterial to the Court's determination on summary judgment.

argue that NaviStone and Harriet Carter should be treated the same under Pennsylvania law (*i.e.*, as a corporation and its agents) such that Popa consented to communications with NaviStone because she intended to communicate with Harriet Carter. Defendants contend that Harriet Carter posted a privacy policy and that Popa's decision not to review the policy, despite being on constructive notice of it, implies consent. For the reasons that follow, the Court will grant Defendants' motion and enter summary judgment in their favor.

I. STANDARD OF REVIEW

Summary judgment is warranted if the Court is satisfied that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a); *see also Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). A fact is material if it must be decided to resolve the substantive claim or defense to which the motion is directed. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). There is a genuine dispute of material fact "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Id.* The Court must view the evidence presented in the light most favorable to the nonmoving party. *Id.* at 255. It refrains from making credibility determinations or weighing the evidence. *Id.* "[R]eal questions about credibility, gaps in the evidence, and doubts as to the sufficiency of the movant's proof[]" will defeat a motion for summary judgment. *El v. Se. Pa. Transp. Auth.*, 479 F.3d 232, 238 (3d Cir. 2007).

II. FACTUAL BACKGROUND

For purposes of this second motion for summary judgment, the parties incorporated the averments in their earlier concise statement and counterstatements of material fact and, in addition, submitted supplemental statements and counterstatements of material fact focusing on the facts relevant to the issue on remand—particularly that of consent under WESCA. In examining the

motion and rendering its decision, the Court finds it unnecessary to restate the factual background regarding the nature of Harriet Carter's website and NaviStone's software, how such software works in the operation of the internet, and other technical aspects of this action. The Court incorporates by reference the factual recitation portion of its previous opinion on summary judgment. (ECF No. 116, pp. 1-4). The Court supplements its recitation of the relevant facts with the following undisputed facts, which specifically relate to the issue before the Court—the question of Popa's consent.

In early 2018, Popa visited Harriet Carter's website, *www.harrietcarter.com*, where she provided her email address, searched for pet stairs, and added one or more items to her online cart. It is not disputed that at all times relevant to this case, Harriet Carter had a privacy policy posted in the footer of its website. (ECF No. 172, p. 19). The privacy policy was presented as a link, labeled "Privacy Statement." (*Id.* at 20). The link was in white, against a blue background. (*Id.*). The parties, including their experts, agree that presenting a link to a privacy policy in the footer of a website was the common practice for commercial websites in 2018. (*Id.*). The parties further agree that in 2018, it would have been a "reasonable conclusion" for a company to believe that "it ought to put the privacy policy link in the footer of its website." (*Id.* at 20-21).

The Harriet Carter privacy policy ("Privacy Statement") broadly address its practices with respect to collection and use of customer information collected from its website. (ECF No. 167-4, pp. 141-43). Under the heading "When I visit HarrietCarter.com, what information is gathered about me and why?" the Privacy Statement states, *inter alia*, "Harriet Carter does collect certain customer information. We use this information to process orders, enhance your shopping experience and communicate with our customers." (*Id.* at 141). The Privacy Statement has a section entitled "What are Cookies and Should I Worry About Them?" that explains what cookies

are and how they are used in connection with the Harriet Carter website. (*Id.*). It explains, for example, that "[o]ur site does use cookies to keep track of your shopping cart. We also use cookies to help make your shopping experience more enjoyable and if you choose to register with us or request to receive email, we will use cookies to deliver content specific to your interests." (*Id.*). The Privacy Statement has a section that addresses the access of third parties to customer information. The heading states, in bold type: "Who Else Has Access to the Information I provide to Harriet Carter.com?" It states, in relevant part:

> We may from time to time contract with third party vendors to serve ads to our customers on our behalf across the Internet or to send our catalogs to customers whom we think may be interested in our products or services. To do this, the vendors will collect anonymous information about your visits to our Web site and your interaction with our products and services. This anonymous information is collected through the use of a cookie or pixel tag—industry standard technology used by most major Web sites. No personally identifiable information is collected in this process. They may also pool the anonymous information that they collect with other sources of information not collected during your visit to our website, which may include your name and mailing address.

(*Id.* at 141-42).[2]

It is not in dispute that Popa visited the Harriet Carter website in early 2018 using the Safari browser on her iPhone. (ECF No. 105, p. 29). She provided her email address, used the search function to look for pet stairs, and added one or more items to a shopping cart. (*Id.*). Popa never completed the purchase.[3]

In Popa's deposition, she testified that she has never reviewed the Privacy Statement:

---

[2] The Harriet Carter/NaviStone Agreement required that Harriet Carter publish via "a clear and conspicuous link" a privacy policy that explained to consumers the information collection and disclosure practices associated with NaviStone's services. (ECF No. 105, p. 28).

[3] Popa no longer has the cell phone that she used to visit the Harriet Carter website. (ECF No. 105, p. 29). As such, she has no record of the cookies associated with either defendant. (*Id.*). In fact, Popa does not recall the exact number of times she visited the website. (ECF No. 172, p. 23). She has no record beyond her recollection of her visit to the Harriet Carter website. (*Id.*).

Q. Did you ever undertake, for your own purposes, a review of the privacy policies of the Harriet Carter website?

A. No, I have not.

Q. Have you ever looked to see whether those privacy policies described the activities of NaviStone?

A. No, I have not.

(ECF No. 167-3, pp. 98-99). Popa testified that, as a matter of practice, she does not review privacy policies:

Q. Did you review any privacy policy that they [a social media carrier] might have had?

A. No.

Q. Why not?

A. I just don't

Q. As a matter of practice, you don't?

A. Correct.

* * *

Q. And when you say you don't review terms and conditions and privacy policies as a matter of practice, is there a reason that underlies that practice?

A. No.

Q. You simply don't, but for no particular reason; is that right?

A. Correct.

(*Id.* at 97-98). Popa further testified that after this lawsuit was filed, she has "skimmed over" privacy policies if they pop-up. (*Id.* at 98). She testified that "If I see the privacy policy pop up on a website, I will skim over it. Usually it's very long, and I don't have time to sit there and read it." (*Id.* at 99-100).

III. ANALYSIS

The Third Circuit remanded the matter for the Court to examine two issues that it previously declined to address; (1) whether Popa can be deemed to have consented to NaviStone's activities pursuant to the Harriet Carter Privacy Statement; and (2) where NaviStone's interception occurred. After supplemental discovery on these issues, Defendants abandoned the issue of where the interception occurred. Their second motion for summary judgment focuses on the issue of consent. Beyond the question of whether Popa should be deemed to have consented due to the operation of the Privacy Statement, Defendants also argue that the nature of the internet, and its use of third-party code, creates implied consent. For the reasons that follow, Defendants' motion will be granted.

A. DEFENDANTS RAISE ISSUES THAT ARE OUTSIDE THE SCOPE OF THE THIRD CIRCUIT'S REMAND AND, CRITICALLY, WITHIN THE SCOPE OF ITS RULING ON WHETHER THERE WAS AN INTERCEPTION UNDER WESCA.

Before addressing the question of whether Popa consented to NaviStone's activities under the terms of the Privacy Statement, Defendants argue that (1) as an agent of Harriet Carter, NaviStone's conduct cannot be viewed as an intercept under WESCA, (ECF No. 166, pp. 17-22); and (2) the nature of the internet itself, with the ubiquity of "cookies" and third-party software, creates implied consent to NaviStone's conduct (*id.* at 22-31). Having carefully reviewed Defendants' arguments, the Court holds that, while not entirely coterminous with the arguments previously presented to the Court and the Third Circuit as to whether an actionable intercept occurred, they are nevertheless precluded by the Third Circuit's decision which is both law of the case and precedent beyond the contours of this action.

1) The fact that NaviStone was Harriet Carter's agent was already before the Court and the Third Circuit. It does not impact the scope of the Third Circuit's decision.

Defendants' first argument addresses the question of whether NaviStone can be deemed to have engaged in an intercept under WESCA. This argument clearly implicates the heartland of the rationale underlying the Third Circuit's decision that a party to a communication cannot be deemed an interceptor under WESCA. In fact, Defendants, in footnotes, specifically take issue with the rationale of the Third Circuit's holding, while recognizing that the holding is the law of the case. Defendants concede that they have raised issues with the Third Circuit's decision only to preserve them for appeal.

Beyond preserving their disagreement with the Third Circuit's rationale, Defendants attempt to distinguish the instant issue from that addressed by the Third Circuit by focusing on the fact that NaviStone was an agent of Harriet Carter, and thus stood in the shoes of Harriet Carter for the purpose of determining whether there was an intercept, or whether NaviStone should be considered an extension by agency of Harriet Carter. Defendants cite to a number of cases for the proposition that where third-party analytics software "functions as an extension of the website itself" it "should be viewed as one in the same for purposes of analyzing a wiretapping claim." (ECF No. 166, p. 20 (internal citations omitted)).

The issues raised by Defendants relating to agency are not distinguishable from the issues presented to and decided by the Third Circuit. It was clear in the parties' arguments to this Court (and in its initial decision on summary judgment) that NaviStone was acting as an agent of Harriet Carter and undertaking its role on behalf, and with permission, of Harriet Carter. (*See* ECF No. 105, p. 5 ("NaviStone considers itself to be acting on behalf of and under the authority of each of its individual clients to which it provides the Services.")); (ECF No. 116, p. 2 ("NaviStone provides its clients—primarily e-commerce retailers—with services that allow them to send direct mail promotions to people visiting their websites. One of those clients is Harrier Carter.")); (ECF

No. 122-2, p. 3 ("But she later discovered that, unbeknownst to her as she was browsing the website, a third-party marketing service Harriet Carter was using, NaviStone, tracked her activities across the site.")). It is undisputed that the Third Circuit was aware that NaviStone was Harriet Carter's agent and working only on Harriet Carter's behalf. No party ever argued or alleged that NaviStone was a hacker or an otherwise unauthorized interloper. The Third Circuit focused its decision not on whether NaviStone was making an intercept of Popa's information as Harriet Carter's agent, but on the fact that Popa did not know that NaviStone was doing so. Defendants' arguments ask the Court to second guess an area already decided by the Third Circuit. Any such analysis by the Court is precluded by the Third Circuit's opinion.

2) Defendants' argument about implied consent to interception arising from the nature of the internet is also covered by the Third Circuit's decision.

Defendants argue that the nature of the internet creates implied consent to the interception of user data. (ECF No. 166, p. 23). They contend that "third-party code is ubiquitous on the internet, " that it is impossible or infeasible to build a website without the use of third-party code, and that neither party's experts were able to identify a single website that does not use third-party resources. (*Id.* at 25). Defendants argue that courts should imply consent to intercepts under WESCA or, otherwise, the operation of the entire internet may run afoul of the Pennsylvania statute. The Third Circuit's opinion contemplated, and unequivocally rejected, this very argument:

> So does this mean that websites can never use cookies or third-party marketing companies to analyze customer data? Though the Defendants try to convince us about the certainty of any number of "parade of horribles," the WESCA is not so unreasonable. It, like the Federal Wiretap Act, includes many exceptions from liability. One is the all-party consent exception, under which it is not unlawful for someone to "intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception." 18 Pa. C.S. §5704(4). Thus if someone consents to the interception of her communications with a website, the WESCA does not impose liability. Here the Defendants obviously consented to the interception. The question is whether Popa did as well.

(ECF No. 122-2, p. 20). The Court will not reexamine issues already addressed by the Third Circuit. It will focus on the issue presented by the Third Circuit on remand—whether Popa consented to NaviStone's activities on the Harriet Carter website.

B. POPA'S WESCA CLAIM FAILS BECAUSE SHE IMPLICITLY CONSENTED TO ANY INTERCEPT BY NAVISTONE, WHICH WAS DISCLOSED IN HARRIET CARTER'S PRIVACY STATEMENT AND READILY ACCESSIBLE TO POPA.

Pursuant to WESCA, "[i]t shall not be unlawful and no prior court approval shall be required under this chapter for: A person to intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception." 18 Pa. C.S. § 5704(4). Pennsylvania courts have repeatedly interpreted the consent provisions of WESCA as establishing an objective standard—looking to whether a reasonably prudent person can be deemed to have consented under the circumstances.

1) The determination of consent under WESCA is based on the objective standard of a reasonably prudent person.

In *Commonwealth v. Byrd*, 235 A.3d 311 (Pa. 2020), the Pennsylvania Supreme Court granted allocatur to examine the standard to be used by courts interpreting the consent provisions of WESCA. *Byrd* discussed whether an inmate had to have actual knowledge that his communications were being recorded to satisfy the consent provisions of WESCA. *Byrd*, 235 A.3d at 317. The trial court suppressed incriminating evidence in communications that occurred between Byrd and a third party during a prison visit. *Id.* at 315-16. While the telephonic communications system used in such visits included a recording at the beginning of use stating that the communications "may be monitored or recorded," the trial court held that the Commonwealth failed to present evidence that Byrd heard the recording, noting that "it is not outside the realm of possibility that [Appellant] did not have the receiver to his ear when the

recording played, and therefore may not have heard it." *Id.* at 316. In other words, the suppression court was looking for evidence of actual knowledge before it would impute consent to Byrd.

The Pennsylvania Supreme Court disagreed with the trial court and held that suppression was not appropriate because actual knowledge is not required under the mutual consent provisions of WESCA. The Court explained:

> [T]he phrase "actual knowledge" does not appear in the statutory language of the mutual consent exception and Appellant fails to argue any basis for its application as the standard. Rather, our case law illustrates that "prior consent" can be demonstrated when the person being recorded "knew or should have known, that the conversation was being recorded." This standard is one of a reasonable person, and not proof of the subjective knowledge of the person being recorded as Appellant advocates.

Id. at 319 (quoting *Commonwealth v. Diego*, 119 A.3d 370, 377 (Pa. Super. 2015)). Because the WESCA mutual consent exception focuses on a reasonable person standard, the Pennsylvania Supreme Court held that it was not necessary to show that Byrd had actual knowledge of the disclosure that his communications may be recorded. *Id.* at 319. Rather, under the reasonable person standard, the Court held that the mere receipt of that disclosure was enough to satisfy the mutual consent requirement. *Id.* at 320.

The Pennsylvania Supreme Court's decision in *Byrd* cited to the decision of the Pennsylvania Superior Court in *Commonwealth v. Proetto*, 771 A.2d 823 (Pa. Super. 2001), which held that the nature of internet communication implies consent on the part of a reasonable person under WESCA's mutual consent provisions. *Proetto*, 771 A.2d at 830. *Proetto* concerned sexually explicit communications between a criminal defendant and a police investigator that he believed was an underage girl. *Id.* at 826. The Superior Court rejected WESCA-based challenges to the defendant's conviction on multiple grounds. First, the Superior Court held that there was no intercept under WESCA because the law enforcement officer was a direct participant to the

communication, even if the defendant believed he was communicating with someone else. *Id.* at 832. Second, and significant to this case, the Superior Court held that the defendant's "email and chat-room communications fall within the mutual consent provision of [WESCA]." *Id.* at 829. In doing so, the Superior Court took a broad approach, holding that a reasonable person provides consent under WESCA based on the very nature of the internet:

> This situation is unlike one in which a party is engaging in a conversation over the telephone. While engaging in a conversation over the telephone, a party would have no reason to believe that the other party was taping the conversation. Any reasonably intelligent person, savvy enough to be using the Internet, however, would be aware of the fact that messages are received in a recorded format, by their very nature, and can be downloaded or printed by the party receiving the message. By the very act of sending a communication over the Internet, the party expressly consents to the recording of the message.

Id. Following the Superior Court's decision, the Pennsylvania Supreme Court granted allocatur on two issues:

> I. Whether the [trial court and Superior Court] erred in failing to suppress certain communications obtained in violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act.
>
> II. Whether the [trial court and Superior Court] erred in failing to suppress certain communications obtained in violation of the United States Constitution and/or the Pennsylvania Constitution.

Commonwealth. v. Proetto, 837 A.2d 1163, 1164 (Pa. 2003). The Supreme Court issued a *per curiam* order affirming the Superior Court's decision. *Id.* ("[T]he Order of the Superior Court is hereby affirmed on the basis of the Superior Court Opinion."). Thus, the Superior Court's opinion represents the position of the Pennsylvania Supreme Court on the issues within the scope of its allocatur grant—which encompasses the Superior Court's decision as to the consent provision of WESCA. *Proetto*, 837 A.2d at 1164 (citing *Commonwealth v. Tilghman*, 673 A.2d 898, 904 (Pa. 1996) ("[A] *per curiam* order affirming the decision of a trial court or one of our intermediate

appellate courts signifies this Court's agreement . . . with [that] tribunal's final disposition of the matter on appeal to us.").

While not expressly addressing WESCA, but relevant to the reasonable person standard, the Third Circuit has made observations about the expectation of privacy in internet activity that is consistent with *Proetto*. In *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 266 (3d Cir. 2016), the Third Circuit observed:

> Most of us understand that what we do on the Internet is not completely private. How could it be? We ask large companies to manage our email, we download directions from smartphones that can pinpoint our GPS coordinates, and we look for information online by typing our queries into search engines. We recognize, even if only intuitively, that our data has to be going somewhere. And indeed it does, feeding an entire system of trackers, cookies, and algorithms designed to capture and monetize the information we generate. Most of the time, we never think about this. We browse the Internet, and the data-collecting infrastructure of the digital world hums along quietly in the background.

In re Nickelodeon, 827 F.3d at 266. Contrary to Defendants' argument that the nature of the internet itself warrants a finding of implied consent to interception under WESCA, and respectful of the Third Circuit's observation that *Nickelodeon* is distinguishable because of WESCA's two-way consent requirement, the Court finds the above-quoted language instructive on the reasonable person standard used to examine implied consent under WESCA. It recognizes that, while the nature of the internet does not confer blanket implied consent to interception under WESCA, a reasonably prudent person has a lower expectation of privacy on the internet than on, for example, a telephone, which lacks the "entire system of trackers, cookies, and algorithms" commonly, if not ubiquitously, implicated in the use of a website. Like the court in *Proetto*, the Court believes that when determining whether a reasonable person can be deemed to consent to an interception under WESCA, it must be mindful of the reality of internet communication and expectations of ordinary people in interacting with the internet.

2) Harriet Carter's Privacy Statement adequately describes NaviStone's activities.

The Court must consider the scope of the alleged consent when evaluating a privacy statement. *Opperman v. Path Inc*, 84 F. Supp. 3d 962, 992 (N.D. Cal. 2015) (citing *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1028 (N.D. Cal. 2014)). In order for a privacy statement to convey consent to an interception, it must disclose the nature of the interception to a reasonable reader. To determine whether Popa consented to an intercept under WESCA, the Court first looks to whether Harriet Carter's website adequately disclosed NaviStone's activities. Not unlike the disclosure of the recording in *Byrd*, the question is whether a reasonable person *could* have been apprised of the complained-of activity. The Court holds that the Privacy Statement adequately discloses that third parties, like NaviStone, may have access to information relating to consumers' activities on the website.

The Privacy Statement makes clear that Harriet Carter uses cookies on its website and that those cookies may track users' activities. The Privacy Statement also includes language that unequivocally reveals that Harriet Carter may share information about users' activities with third parties. The Privacy Statement has a heading which highlights the nature of the operative language, stating: "Who Else Has Access to the Information I provide to Harriet Carter.com?" The relevant section of the Privacy Statement states:

> We may from time to time contract with third party vendors to serve ads to our customers on our behalf across the Internet or to send our catalogs to customers whom we think may be interested in our products or services. To do this, the vendors will collect anonymous information about your visits to our Web site and your interaction with our products and services. This anonymous information is collected through the use of a cookie or pixel tag—industry standard technology used by most major Web sites. No personally identifiable information is collected in this process. They may also pool the anonymous information that they collect with other sources of information not collected during your visit to our website, which may include your name and mailing address.

(ECF No. 167-4, p. 142). The Court holds that the plain language of the Privacy Statement adequately discloses that type of conduct that forms the basis of Popa's WESCA claim. Specifically, it discloses (1) that Harriet Carter may contract with third parties for marketing purposes; (2) that these vendors may use cookies to collect information about the user's visit to the website and interaction with its products and services; and (3) that no personally identifiable information is collected in the process; and (although not directly implicated by Popa's claim), (4) that this information may be pooled with other information not collected from the website visit. (*See id.*) The Privacy Statement provides sufficient information to alert a reasonably prudent visitor to the Harriet Carter website of the critical issue for a WESCA claim—that third parties, like NaviStone, may collect data relating to the visitor's conduct on the website.[4]

3) The record establishes that Popa consented to NaviStone's activities on the Harriet Carter website.

In this case, Popa does not allege, and the record does not establish, that she actually reviewed the Privacy Statement. No record evidence exists that during the visit(s) relevant to her claim she looked for the Privacy Statement but was unable to find or open it. Indeed, she testified that, as a general matter of practice, she does not review privacy policies. (ECF No. 167-3, pp. 97-98). Even after initiating this action, Popa admitted that she has never accessed or reviewed the Privacy Statement. (*Id.* at 98-99). The record does not show, therefore, that Popa had actual knowledge of the terms of the Privacy Statement. As in *Byrd*, the question is not whether Popa

[4] Contrary to Popa's argument, compliance with WESCA does not require that the Privacy Policy reveal granular details about the identity of the "third parties" or the specific type of cookies used on the Harriet Carter website to confer information needed to establish consent. Rather, WESCA focuses on the event of an interception rather than the specific details thereof. Using the example of the facts in *Byrd*, the exact means by which the communications would be recorded (i.e., tape, CD, or electronic file) was immaterial to the issue of consent. Likewise, the identity of the disclosed recorder was also immaterial. The important point with respect to WESCA is the fact that a recording could occur was disclosed.

had actual knowledge, but rather, whether a reasonable person can be found to have provided implied consent to the alleged interception by her actions. To make this determination, the Court must critically examine the circumstances of Popa's interaction with Harriet Carter's website. It must consider whether a reasonable person in her circumstance could be charged with implicit knowledge of the disclosures in the Privacy Statement. This turns on the visibility and accessibility of the Privacy Statement to an ordinary user.

The question of whether a reasonable person would have had sufficient notice of Harriet Carter's Privacy Statement follows the type of analysis commonly employed by courts to determine whether a user assented to a website's contractual terms and conditions by continued use of the website. Courts have recognized that there are two general methods of posting terms and conditions on a website:

> Contracts formed on the Internet come primarily in two flavors; "clickwrap" (or "click-through") agreements, in which website users are required to click on an "I agree" box after being presented with a list of terms and conditions of use; and "browsewrap" agreements, where a website's terms and conditions of use are generally posted on the website via a hyperlink at the bottom of the screen.
>
> "Unlike a clickwrap agreement, a browsewrap agreement does not require the user to manifest assent to the terms and conditions expressly. . . [a] party instead gives his assent simply by using the website."

Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1175-76 (9th Cir. 2014) (quoting *Hines v. Overstock.com, Inc.*, 668 F. Supp. 2d 362, 366-67 (E.D. N.Y. 2009)). "A 'browsewrap agreement' allows the user 'to view the terms of the agreement but does not require the user to take any affirmative action before the Web site performs its end of the contract.'" *Freeplay Music, LLC v. Dave Arbogast Buick—GMC, Inc.*, No. 3:17-CV-42, 2019 WL 4647305, at *10 (S.D. Ohio Sept. 24, 2019) (internal citations omitted). It is undisputed that Harriet Carter's Privacy Statement took

the form of a browsewrap agreement and, while it was visible and accessible, visitors were not required to click or otherwise express affirmative consent to its terms.

Courts consistently enforce browsewrap agreements when users have actual notice. *Nguyen*, 763 F.3d at 1176; *see also Register.com Inc. v. Verio, Inc.*, 356 F.3d 393, 401 (2d. Cir. 2004); *Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 WL 21406289, at *1 (C.D. Cal. Mar. 7, 2003). If there is no evidence of actual knowledge, the enforceability of a browsewrap agreement turns on whether the website placed a reasonably prudent user on inquiry notice of its terms. *Nguyen*, 763 at 1177 (citing *Specht v. Netscape Common's Corp.,* 306 F.3d 17, 30 (2d. Cir. 2002)). The content of a webpage and privacy agreement page determine whether a defendant adequately provides inquiry notice. *Id.* (citing *Be In, Inc. v. Google, Inc.*, 2013 WL 5568706, at *1 (N.D. Cal. Oct. 9, 2013)).

Courts have generally held that "constructive knowledge alone is sufficient to establish consent to 'browsewrap' terms and conditions when the website host placed the notice of the terms and agreements 'prominently' and provided 'easy access' to the full terms." *Freeplay Music*, 2019 WL 4647305, at *11 (quoting *Snap-On Bus. Sols. Inc. v. O'Neil & Assocs., Inc.,* 708 F. Supp. 2d 669, 682 (N.D. Ohio 2010)). Citing to the Ninth Circuit's decision in *Nguyen*, the Third Circuit has explained that "[t]here is an evolving body of caselaw regarding whether the terms and conditions in browsewrap agreements are enforceable, often turning on whether the terms or a hyperlink to the terms are reasonably conspicuous on the webpage." *James v. Global Tellink Corp.*, 852 F.3d 262, 267 (3d. Cir. 2017) (internal citations omitted). The Third Circuit observed that such terms will likely not be enforced "[w]hen terms are in obscure sections of a webpage that users are unlikely to see." *Id.* (citing *Specht*, 306 F.3d at 30-32). The Second Circuit similarly observed that "clarity and conspicuousness" of terms are "important in securing informed

consent." *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 233 (2d. Cir. 2016); *see also Meyer v. Uber Technologies, Inc.*, 868 F.3d 66, 75-76 (2d. Cir. 2017) (same).

The Court finds *HealthplanCRM LLC. v. AvMed, Inc*, 458 F. Supp. 3d 308 (W.D. Pa. 2020) instructive on this issue. In *HealthplanCRM*, the issue was whether a website user was bound by the terms of an arbitration clause contained in a browsewrap agreement of a website. *HealthplanCRM*, 458 F. Supp. at 331. The district court examined many of the cases cited above and explained that terms in a browsewrap agreement will be enforced provided that the agreement was reasonably conspicuous or, conversely, was not linked in "obscure sections of a webpage that users are unlikely to see." *Id.* at 332 (citing *James*, 852 F.3d at 267). The party seeking to avoid the arbitration agreement argued that the browsewrap agreement was not sufficiently conspicuous:

> Here, the relevant browsewrap language is found on the log-in page of Cavulus's software platform. Cavulus attaches a screenshot of the log-in page to its complaint as an exhibit, and NTT does not dispute the screenshot's authenticity. The log-in page consists of a box to type in a user ID and password and then, about one inch below that box, a sentence reading: "Use of Cavulus constitutes acceptance of the End User License Agreement," containing a hyperlink to the Agreement itself.
>
> * * *
>
> NTT argues that the browsewrap End-User Agreement is not sufficiently "conspicuous" to be enforced, because the link to the End-User Agreement is "in small font, positioned close to a large paragraph of text in the same small font, and is far enough below the log-in boxes and button so as not to command the viewer's attention."

Id. at 332-33 (internal citations omitted). The district court rejected the contention that the browsewrap agreement was insufficiently conspicuous:

> The Court cannot agree with this characterization. The link to the End-User Agreement appears no more than an inch below the log-in boxes, and it is both above and set apart from the "large paragraph" of text NTT references (which is itself only six sentences long). The link is not concealed at the bottom of a webpage or hidden in fine print. What's more, the blue hyperlink to access the full End-User Agreement stands out against the white background of the log-in page and appears

> in a sentence which straightforwardly advises the user that "[u]se of Cavulus constitutes acceptance" of the linked agreement.

Id. at 333.

The Court finds it significant that the *HealthplanCRM* court found that the arbitration agreement was sufficiently conspicuous so as to be enforced when the hyperlink was titled "End User License Agreement." *See id.* at 315. This title gave no indication of the existence of an arbitration clause. Nevertheless, the court held that the visibility of the link was sufficient to create constructive notice of the contents of that link—including an arbitration clause. *Id.* at 337. This stands in contrast to the instant case, which asks whether Harriet Carter's website was sufficient to impart constructive notice of the privacy-related terms of a hyperlink entitled "Privacy Statement."

The Court holds that the Privacy Statement on Harriet Carter's website was "reasonably conspicuous on the webpage" so as to charge Popa with "'constructive notice' that continued use [constituted] acceptance of the agreement." *HealthplanCRM*, 458 F. Supp. at 331 (quoting *James*, 852 F.3d at 267). It is undisputed that, at the time relevant to this case, Harriet Carter had a hyperlink labeled "Privacy Statement" in the footer of every page of its website. (ECF No. 172, p. 20). The hyperlink was in white font contrasting against a blue background. (*Id.*). In addition to this location at the center and bottom of each page, a link to the privacy statement could be found in the drop-down menu on the left side of the website directly below "Email Us." (ECF No. 167-4, p. 141). The Court holds that, based on the appearance and layout of Harriet Carter's website, the Privacy Statement was reasonably conspicuous. It was not, for example, linked in "obscure sections of a webpage that users are unlikely to see." *HealthplanCRM*, 458 F. Supp. at 332 (citing *James*, 852 F.3d at 267). Nor were the relevant terms concerning the policy, as the arbitration clause in *HealthplanCRM*, included in a hyperlink generically labeled "terms of use"

or the like. Rather the link was specifically labeled "Privacy Statement." Popa, or any other user, could have easily seen the link and understood exactly what it contained.

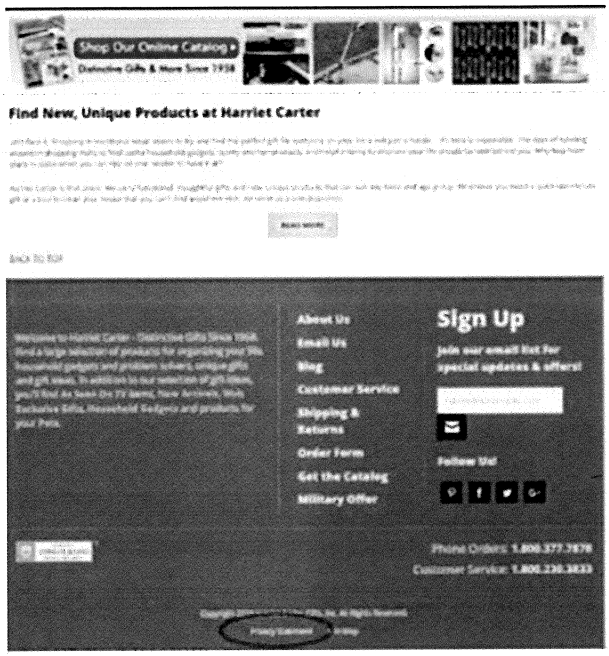
The record also establishes that the placement and appearance of the Privacy Statement on the Harriet Carter website was in line with common usage in 2018. Popa's own expert testified that it was common for privacy policies to be placed on the footer of the websites:

> Q. Is it fair to say that the common practice at that point was to put links to privacy policies in the footers of websites?
>
> A. That was a common practice, certainly.

(ECF No. 167-4, p. 41-42 ("But I do know that it was—that it is a—a common practice to put it in the footer.")). To be clear, whether Harriet Carter's manner of displaying its Privacy Statement was commonplace in 2018 is not independently dispositive. It is, however, instructive. Where the manner of posting a privacy policy was consistent with common industry practice, and the appearance of the language was visible and not hidden in an obscure place on the website, a court should—and this Court is—hesitant to find that the posted terms were incapable of conveying constructive notice.

When viewing the record as a whole, the Court holds that the Privacy Statement is enforceable. Popa's decision not to review its terms does not permit her to avoid the implication of those terms. The hyperlink to the Privacy Statement was reasonably conspicuous. It was displayed in a white contrasting font against a blue background on the bottom of every page of the website[5]:

[5] (ECF No. 167-3, p. 52). The Privacy Statement, in white font against the blue background, is circled in red at the footer of the website.



Further, unlike the generically titled "end user license agreement" in *HealthplanCRM*, the title of the Privacy Statement gave an express indication of the contents of the hyperlink. The Privacy Statement adequately discloses that third parties, such as NaviStone, may access information relating to user activities on Harriet Carter's website. The Court holds that these factors compel a finding that a reasonable person in Popa's position had constructive notice of the terms of the Privacy Statement as a matter of law. As in *Byrd*, the Court holds that Popa constructively consented to any interception effectuated by NaviStone. There was, therefore, no violation of WESCA and summary judgment in Defendants' favor is warranted.[6]

[6] The Court rejects Popa's contention that the presence of NaviStone's program means that merely visiting Harriet Carter's website would give rise to an actionable interception under WESCA before she, or any reasonable user, had a chance to view the terms of the Privacy Statement. This argument is incorrect. To the extent that Popa was concerned about privacy, she could have immediately reviewed the Privacy Statement and, if concerned, left the page. This is no different than if someone who received the warning in *Byrd* hung up the phone after hearing the recording. The mere fact that a user visits Harriet Carter's website is not protected by WESCA any more than that of a caller who uses a phone to reach a number, and then hangs up after being warned of an interception and/or recording. The caller's number may show up, and even be recorded, on a caller identification system, but an intercept has not occurred. WESCA only applies to "contents" of communications, which it defines as "information concerning the substance, purport, or meaning

IV. CONCLUSION

For the foregoing reasons, Defendants' motion for summary judgment will be granted and judgment will be entered in their favor. Orders of Court will follow.

BY THE COURT:

WILLIAM S. STICKMAN IV
UNITED STATES DISTRICT JUDGE

3/24/25
Dated

of that communication." 18 Pa. C.S. § 5702. Accessing the Harriet Carter webpage, visiting the Privacy Statement, and then leaving the site does not lead to the interception of "content" under WESCA.